CLAIMS

What is claimed is:

1. An electronic transaction device comprising:

a transaction device identifier, the identifier providing no apparent identification of a user authorized to use the electronic transaction device;

communication logic configured to communicate the transaction device identifier to a system to perform a transaction, the system comprising a secure mechanism for correlating the device identifier and user; and

a detachable memory device configured to include a public storage area and a private storage area, wherein the private storage area is to store confidential data that is to be encrypted with a key that is stored within memory of the electronic transaction device.

2. The electronic transaction device as set forth in claim 1, wherein the public storage area of the detachable memory device is to be accessible without the key from the user transaction device.

3. The electronic transaction device as set forth in claim 1, wherein the private storage area comprises a number of private storage areas and wherein different keys for accessing each of the number of private storage areas are to be stored in the electronic transaction device.

4. The electronic transaction device as set forth in claim 3, wherein the number of private storage areas is associated with different levels of encryption.

5. The electronic transaction device as set forth in claim 1, wherein a data protection mode signal is operable to be wirelessly transmitted to the electronic transaction device to cause the electronic transaction device to remove the key that is to encrypt the private storage area of the memory storage device.

6. The electronic transaction device as set forth in claim 5, wherein the data protection mode signal is to be wirelessly transmitted to the electronic transaction device using a communication system.

7. The electronic transaction device as set forth in claim 5, wherein a key-located mode signal is operable to be wirelessly transmitted to the electronic transaction device to cause the electronic transaction device to store the key for encryption of the private storage area, wherein the key-located mode signal is to include the key for encryption of the private storage area.

8. The electronic transaction device as set forth in claim 1, wherein the transaction device is selected from the group consisting of a privacy card, digital wallet, and a privacy card configured to be coupled to a digital wallet.

9. The electronic transaction device as set forth in claim 1, wherein the security logic is selected from logic to confirm an identification selected from the group consisting of a PIN code and fingerprint.

10. The electronic transaction device as set forth in claim 1, wherein the communication logic is selected from the group consisting of a smart card chip interface, contactless connection, magnetic stripe and wireless connection.

11. The electronic transaction device as set forth in claim 1, further comprising a transaction history storage area configured to store transaction records.

12. The electronic transaction device as set forth in claim 1, further comprising a financial data storage area configured to store information selected from the group consisting of eCoupons, account balances and other data used during a transaction.

13. The electronic transaction device as set forth in claim 1, wherein the communication logic is configured to accept direct marketing information.

14. An electronic transaction device comprising:

a processor;

an internal memory coupled to the processor, wherein a transaction device identifier is to be stored within the internal memory, the transaction device identifier to provide no apparent identification of a user authorized to use the electronic transaction device;

a peripheral port coupled to the processor and the internal memory, wherein the peripheral port is operable to be communicatively coupled to an external memory storage device, wherein the external memory storage device is configured to include a public storage area and a private storage area, wherein the private storage area is to store confidential data that is to be encrypted with a key that is stored within the internal memory of the electronic transaction device; and

an electronic commerce process to be executed by the processor to cause the processor to conduct an electronic commerce transaction with a vendor using data stored in the public storage area of the detachable memory storage device.

15. The electronic transaction device as set forth in claim 14, wherein the public storage area of the detachable memory device is to be accessible without the key from the user transaction device.

16. The electronic transaction device as set forth in claim 14, wherein the private storage area comprises a number of private storage areas and wherein different keys for accessing each of the number of private storage areas are to be stored in the electronic transaction device.

17. The electronic transaction device as set forth in claim 16, wherein the number of private storage areas is associated with different levels of encryption.

18. The electronic transaction device as set forth in claim 14, further comprising a wireless communication interface coupled to the processor to receive a data protection mode signal and wherein the processor removes the key that is to encrypt the private storage area of the memory storage device in response to receipt of the data protection mode signal.

19. The electronic transaction device as set forth in claim 14, further comprising a wireless communication interface coupled to the processor to receive a key-located mode signal that includes the key for encryption of the private storage area, and wherein the processor stores the key for encryption of the private storage area in response to receipt of the key-located mode signal.

20. An electronic system comprising:

a user transaction device that provides a device identifier when coupled to a transaction terminal, wherein said transaction terminal is configured to indicate that a transaction is to be performed when coupled to the user transaction device; and

a transaction privacy clearinghouse (TPCH), coupled selectively to the user transaction device when the transaction is to be performed, said TPCH coupled to receive the device identifier and accessible data, wherein the accessible data is to be stored in a public storage area of a memory storage device that can be communicatively coupled to the user transaction device, said TPCH authorizing the transaction based upon the device identifier and the accessible data that includes account information of a user that is authorized to use the user transaction device,

wherein the transaction is authorized without providing the identity of the user to the transaction terminal and wherein the memory storage device is to include a private storage area for storage of confidential data such that the private storage area is to be encrypted with a key that is to be stored in the user transaction device.

21. The electronic system as set forth in claim 20, wherein the memory storage device is detachable from the user transaction device.

22. The electronic system as set forth in claim 20, and wherein the public storage area of the memory storage device is to be accessible without the key from the user transaction device.

23. The electronic system as set forth in claim 20, wherein the private storage area comprises a number of private storage areas and wherein different keys for accessing each of the number of private storage areas are to be stored in the user transaction device.

24. The electronic system as set forth in claim 23, wherein the number of private storage areas are associated with different levels of encryption.

25. The electronic system as set forth in claim 20, wherein a data protection mode signal is operable to be wirelessly transmitted to the user transaction device to cause the

user transaction device to remove the key that is to encrypt the private storage area of the memory storage device.

26. The electronic system as set forth in claim 25, wherein the data protection mode signal is to be wirelessly transmitted to the user transaction device using a communication system.

27. The electronic system as set forth in claim 25, wherein a key-located mode signal is operable to be wirelessly transmitted to the user transaction device to cause the user transaction device to store the key for encryption of the private storage area, wherein the key-located mode signal is to include the key for encryption of the private storage area.

28. The electronic system as set forth in claim 20, wherein the transaction terminal is selected from the group consisting of a point of sale (POS) terminal, home computer system, bank automatic teller machine (ATM) terminal, digital television, Internet Appliance, and personal POS terminal.

29. The electronic system as set forth in claim 20, wherein the transaction device is selected from the group consisting of a privacy card, digital wallet, and a privacy card configured to be coupled to a digital wallet.

30. The electronic system as set forth in claim 20, wherein the TPCH is further configured to selectively couple to a financial institution.

31. The electronic system as set forth in claim 20, wherein the TPCH further comprises a financial institution.

32. The electronic system as set forth in claim 20, wherein the TPCH comprises a secure database of transaction device information and user information, said database accessed for authorizing a transaction.

33. The electronic system as set forth in claim 20, wherein the TPCH is configured to interface to a financial processing system configured to perform financial transactions associated with the transaction.

34. The electronic system as set forth in claim 33, wherein the financial processing system is configured to transfer funds in an amount associated with the transaction from a user's account to an account of a vendor of the transaction.

35. The electronic system as set forth in claim 20, further comprising a distribution system configured to provide a product of the transaction to the user.

36. The electronic system as set forth in claim 20, wherein the TPCH further comprises a distribution system configured to provide a product of the transaction to the user.

37. The electronic system as set forth in claim 20, wherein the TPCH is further configured to perform operations selected from the group consisting of data mining based upon transactions performed and direct marketing to a transaction device of the user.

38. The electronic system as set forth in claim 37, wherein results of data mining are provided without identification of the user and direct marketing is performed without identifying the user.

39. The electronic system as set forth in claim 20, wherein the transaction terminal, transaction device and TPCH are further configured to verify the legitimacy of each other.

40. A method for permitting a user to conduct electronic commerce transactions, the method comprising:

in a secure server, maintaining an association between the user and a transaction device using a transaction device identifier that corresponds to the user, wherein the transaction device is communicatively coupled to a detachable memory storage device having a public storage area and a private storage area, the private storage area being encrypted with a key that is stored in the transaction device; and

conducting an electronic commerce transaction with a vendor using data stored in the public storage area of the detachable memory storage device.

41. The method of claim 40, wherein the private storage area comprises a number of private storage areas and wherein different keys for accessing each of the number of private storage areas are to be stored in the transaction device.

42. The method of claim 41, wherein the number of private storage areas are associated with different levels of encryption.

43. The method of claim 40, wherein a data protection mode signal is operable to be wirelessly transmitted to the transaction device to cause the transaction device to remove the key that is to encrypt the private storage area of the memory storage device.

44. The method of claim 43, wherein a key-located mode signal is operable to be wirelessly transmitted to the transaction device to cause the transaction device to store

the key for encryption of the private storage area, wherein the key-located mode signal is to include the key for encryption of the private storage area.

45. The method of claim 40, wherein the electronic commerce transaction is conducted without requiring the user to reveal personal identification information to the vendor.

46. The method of claim 40, wherein a set of personal identification information corresponding to the user is obtained and associated to the transaction device identifier upon a registration of the transaction device.

47. The method of claim 46, wherein pursuant to the electronic commerce transaction, the delivery of content to the user is initiated using the set of personal identification information.

48. The method of claim 40, wherein pursuant to the electronic commerce transaction, the delivery of content to the user is initiated using the device identifier.

49. The method of claim 40, wherein pursuant to the electronic commerce transaction, the delivery of content to the user is performed without providing personal information of the user.

50. A machine-readable medium that provides instructions for permitting a user to conduct electronic commerce transactions, which when executed by a machine, cause said machine to perform operations comprising:

in a secure server, maintaining an association between the user and a transaction device using a transaction device identifier that corresponds to the user, wherein the transaction device is communicatively coupled to a detachable memory storage device

having a public storage area and a private storage area, such that the private storage area is encrypted with a key that is stored in the transaction device; and

conducting an electronic commerce transaction with a vendor using data stored in the public storage area of the detachable memory storage device.

51. The machine-readable medium of claim 50, wherein the private storage area comprises a number of private storage areas and wherein different keys for accessing each of the number of private storage areas are to be stored in the transaction device.

52. The machine-readable medium of claim 51, wherein the number of private storage areas are associated with different levels of encryption.

53. The machine-readable medium of claim 50, wherein a data protection mode signal is operable to be wirelessly transmitted to the transaction device to cause the transaction device to remove the key that is to encrypt the private storage area of the memory storage device.

54. The machine-readable medium of claim 53, wherein a key-located mode signal is operable to be wirelessly transmitted to the transaction device to cause the transaction device to store the key for encryption of the private storage area, wherein the key-located mode signal is to include the key for encryption of the private storage area.

55. The machine-readable medium of claim 50, wherein the electronic commerce transaction is conducted without requiring the user to reveal personal identification information to the vendor.

56. The machine-readable medium of claim 50, wherein a set of personal identification information corresponding to the user is obtained and associated to the transaction device identifier upon a registration of the transaction device.

57. The machine-readable medium of claim 56, wherein pursuant to the electronic commerce transaction, the delivery of content to the user is initiated using the set of personal identification information.

58. The machine-readable medium of claim 50, wherein pursuant to the electronic commerce transaction, the delivery of content to the user is initiated using the device identifier.

59. The machine-readable medium of claim 50, wherein pursuant to the electronic commerce transaction, the delivery of content to the user is performed without providing personal information of the user.

60. The machine-readable medium of claim 50, further comprising contacting a financial processing system configured to transfer funds in an amount associated with the transaction from the user's account to an account of a vendor of the transaction.

61. The machine-readable medium of claim 60, wherein the financial processing system does not know the user's personal information.

62. The machine-readable medium of claim 60, wherein the financial processing system does not know subject information of the transaction.

63. The machine-readable medium of claim 50, further comprising performing data mining operations related to the transaction.

64. The machine-readable medium of claim 50 further comprising performing direct marketing to the user utilizing the transaction device as the receiver of marketing information.